PERSONAL SUBMISSION

Comments on NIST CSWP 50 IPD

SUBMITTED BY	**Zen Dodd**
SUBMITTED	**03 May 2026**
RECIPIENT	**National Institute of Standards and Technology**
DOCUMENT	**NIST CSWP 50 IPD**

I make these comments in my personal capacity.

These comments concern NIST CSWP 50 IPD, Small Business Cybersecurity: Non-Employer Firms.

My comments focus on practical implementation paths for non-employer firms, account and recovery-channel inventory, SaaS and vendor dependency risk, privacy hygiene, AI-use caution, incident readiness and plain-language security guidance.

Comment 1 - General

Location: Executive Summary / 1. Introduction / vi, 1

Comment and rationale: The draft is well targeted to non-employer firms but the intended audience would benefit from a more explicit time-constrained implementation path. Solo operators often have limited time, no dedicated IT function and must decide what to do first, not simply what to consider. Rationale: The document correctly notes that non-employer firms have minimal IT complexity and limited resources. A clear prioritisation path would reduce cognitive load and increase the likelihood that owners complete the most protective actions first.

Proposed change: Add a short “first 60 minutes / first day / first month” quick-start path near the introduction. For example: first secure email, banking, password manager and business-critical SaaS accounts; then inventory assets and backups; then document legal/contractual obligations and incident contacts.

Comment 2 - Technical

Location: 1. Introduction / 2

Comment and rationale: The basic asset inventory should treat accounts and recovery channels as first-class assets, not only hardware, software, data and services. Rationale: For many non-employer firms, compromise of a primary email account, phone number, password manager, cloud account, domain registrar, payment processor or accounting platform is more damaging than compromise of a single endpoint. Account recovery paths are often the easiest route for attackers and should be inventoried explicitly.

Proposed change: Expand Table 1 and Appendix G to include account owner, administrator account, recovery email/phone, MFA type, recovery-code storage location, criticality and whether the account can reset other business accounts.

Comment 3 - Technical

Location: 1. Introduction / 3

Comment and rationale: The notional architecture is useful but it should more prominently represent SaaS, identity and payment dependencies. Rationale: A modern non-employer firm is often more dependent on cloud-hosted systems than local infrastructure. Email, accounting, online banking, CRM, cloud storage, social media, domain/DNS, storefront and payment processors are high-value assets and common compromise paths.

Proposed change: Revise or supplement Figure 2 with a cloud/SaaS-centric architecture view showing primary email, identity provider, password manager, online banking, domain registrar/DNS, website/storefront, cloud storage, accounting/tax software, payment processor, social media and device backups.

Comment 4 - General

Location: 1. Introduction / 4

Comment and rationale: The list of best practices is strong but it could be made more operational by identifying the highest-priority accounts to secure first. Rationale: “Enable phishing-resistant MFA on all accounts that offer it” is correct but solo operators need a starting order. Business email, password managers, banking, tax/accounting, domain registrar, website/storefront, payment processors and cloud storage should be prioritised because they enable cascading compromise.

Proposed change: Add a small priority table titled “Secure these accounts first” with tiers such as: Tier 1 - email, password manager, banking, domain/DNS, cloud storage; Tier 2 - accounting/tax, payment processor, website/storefront, social media; Tier 3 - other business SaaS.

Comment 5 - Technical

Location: 1. Introduction / 5

Comment and rationale: The privacy discussion is valuable but should provide one or two concrete low-effort privacy controls for non-employer firms. Rationale: The draft correctly notes that cybersecurity risk management is not sufficient to manage privacy risk and gives data retention as an example. A non-employer firm may still hold customer information, identity documents, invoices, health data, tax records or client files. Practical data minimisation and retention guidance would help owners reduce breach impact.

Proposed change: Add a small “minimum privacy hygiene” callout: collect only what is necessary; know where customer/client personal data is stored; set retention periods; delete stale data; avoid storing identity documents unless required; and avoid putting sensitive client data into unapproved AI, analytics or SaaS tools.

Comment 6 - Technical

Location: 1. Introduction / 5

Comment and rationale: The text mentions emerging technologies such as artificial intelligence but the document should address the practical cybersecurity and privacy risks of AI use by sole operators. Rationale: Non-employer firms may use generative AI tools for email, contracts, customer support, coding, marketing or document analysis. The main practical risks include accidental disclosure of client data, use of unapproved browser extensions, malicious AI-generated phishing, dependency on unaudited tools and storing business-sensitive prompts or outputs.

Proposed change: Add a short AI-use note: do not paste customer/client secrets, credentials, legal documents, health information, tax data, source code or unpublished business plans into AI tools unless the owner understands the tool’s retention, training, access and confidentiality terms.

Comment 7 - Technical

Location: 3.1 Govern Function / 9

Comment and rationale: The supplier and third-party risk guidance should include a concrete minimum set of vendor questions for very small firms. Rationale: Contracts are a useful vehicle for managing risk but many non-employer firms lack leverage or legal support. They need plain-language questions that can be used with SaaS providers, MSPs, web developers, bookkeepers, payment processors and cloud platforms.

Proposed change: Add a “minimum vendor questions” box: Does the service support MFA? Who can access my data? How do I export my data? How are backups handled? How fast will I be notified of a breach? What happens if I stop paying? Can subcontractors access data? Is there an audit or security page? How do I delete data?

Comment 8 - General

Location: 3.1 Govern Function / 9

Comment and rationale: The cyber insurance section should more clearly state that insurance is not a substitute for basic controls and incident readiness. Rationale: Non-employer firms may incorrectly treat cyber insurance as equivalent to security. Insurance may impose requirements, exclusions, preferred vendors, breach-notification duties or minimum controls. Owners should understand coverage before an incident rather than discovering exclusions during a crisis.

Proposed change: Add guidance to record policy requirements, exclusions, insurer contact details, preferred incident response providers, ransomware/payment coverage limits and any minimum controls required to maintain coverage.

Comment 9 - Technical

Location: 3.2 Identify Function / 10

Comment and rationale: The inventory guidance should explicitly include external service dependencies and business continuity dependencies. Rationale: For a non-employer firm, outage or account lockout at an ISP, cloud storage provider, payment processor, website host, domain registrar, app store, marketplace or social media platform can stop revenue even if local devices are secure.

Proposed change: Expand the asset inventory guidance to include dependencies such as ISP, domain registrar, DNS provider, hosting provider, payment processor, marketplace/storefront, cloud storage, email provider, accounting software and customer communication channels.

Comment 10 - Technical

Location: 3.2 Identify Function / 10

Comment and rationale: The incident response plan guidance should include an offline or out-of-band copy requirement. Rationale: If the plan is stored only in the same cloud account, password manager or laptop affected by an incident, the owner may not be able to access contacts, recovery codes, insurer instructions, legal obligations or recovery steps when needed most.

Proposed change: Recommend keeping a printed or offline copy of key incident contacts and recovery steps including bank fraud contact, insurer, legal/regulatory contacts, email provider, domain registrar, cloud provider, MSP/IT contact and law enforcement reporting links.

Comment 11 - Technical

Location: 3.2 Identify Function / 10

Comment and rationale: The data sanitisation guidance is too device-centred and should also cover cloud and SaaS data disposal. Rationale: Non-employer firms increasingly store customer and business information in SaaS platforms rather than only on local drives. Risk remains if stale data persists in cloud storage, email, CRM, accounting tools, shared folders, support tickets, exports, backups or abandoned SaaS accounts.

Proposed change: Add cloud/SaaS disposal guidance: close unused accounts, revoke third-party integrations, delete old exports, remove stale shared links, review email/cloud retention, export needed records before account closure and confirm deletion or retention terms with the provider.

Comment 12 - Technical

Location: 3.2 Identify Function / 10-11

Comment and rationale: The risk documentation section should include business email compromise, invoice fraud, account takeover and SIM-swap/phone-number takeover as common risks. Rationale: The document covers phishing and ransomware well but many non-employer firms are harmed through payment redirection, fraudulent invoices, compromised email, malicious mailbox forwarding rules, social media takeover or phone-number takeover.

Proposed change: Add these as example threat events in the risk worksheet and phishing discussion: attacker changes payment details; compromised email sends fraudulent invoice; attacker adds mailbox forwarding rule; attacker takes over social media/storefront account; attacker ports phone number and bypasses SMS recovery.

Comment 13 - Technical

Location: 3.3 Protect Function / 12

Comment and rationale: The least-privilege section should mention OAuth applications, API keys, shared links and delegated SaaS access. Rationale: Solo operators may not have employees but they often grant external apps, plugins, bookkeepers, developers, marketing tools, browser extensions or automation services access to high-value accounts. These access paths can bypass normal password hygiene.

Proposed change: Add guidance to periodically review connected apps, OAuth grants, API keys, shared folders, public links, delegated mailbox access, website plugins and third-party integrations; remove anything no longer needed.

Comment 14 - Technical

Location: 3.3 Protect Function / 12

Comment and rationale: The default-password guidance should explicitly include router remote administration, printer administration, cameras, IoT devices and firmware. Rationale: Changing the default password is necessary but not always sufficient. Small-office routers and network printers may expose remote management, weak Wi-Fi settings, outdated firmware, insecure protocols or cloud administration features.

Proposed change: Add guidance to disable unnecessary remote administration, update router and printer firmware, use WPA2/WPA3 with a strong Wi-Fi passphrase, separate guest/family devices where feasible and record these checks in the asset inventory.

Comment 15 - Technical

Location: 3.3 Protect Function / 12

Comment and rationale: The patching section should address unsupported/end-of-life software and update scope beyond operating systems. Rationale: Automatic updates are important but owners also need to know when software or devices no longer receive security updates. Browsers, browser extensions, website CMS/plugins, router firmware, printer firmware, mobile apps, tax/accounting software and storefront plugins can all be attack paths.

Proposed change: Add guidance to identify end-of-life software/devices, remove unsupported apps, update browser extensions and website plugins and replace devices or services that no longer receive security updates.

Comment 16 - Technical

Location: 3.3 Protect Function / 13

Comment and rationale: The backup guidance should more clearly cover cloud/SaaS data and restoration testing frequency. Rationale: Many non-employer firms assume SaaS providers automatically provide recoverable backups. In practice, a provider may not support customer-level restore, may not protect against accidental deletion or may not recover data after account takeover or non-payment.

Proposed change: Add guidance to identify what SaaS/cloud data can be exported, how often to export it, where exports are stored, whether backups are protected from ransomware/account takeover and when restore tests should be performed. Include examples such as accounting data, customer lists, website content, cloud documents and password manager vault emergency export policies.

Comment 17 - Technical

Location: 3.3 Protect Function / 13-14

Comment and rationale: The MFA guidance is strong but it should include recovery-code and account-recovery hygiene. Rationale: MFA is often undermined through weak recovery paths. Non-employer firms should know that recovery email accounts, phone numbers, recovery codes, helpdesk procedures and backup authenticators are part of the authentication system.

Proposed change: Add guidance to store recovery codes securely, protect recovery email and phone accounts, prefer phishing-resistant MFA where available, avoid SMS for highest-value accounts where better options exist, register backup security keys/passkeys where feasible and document recovery procedures for critical accounts.

Comment 18 - Technical

Location: 3.3.1 Protect Your Business from Phishing / 14

Comment and rationale: The phishing section should include business email compromise and invoice/payment redirection examples. Rationale: Non-employer firms often operate through email, invoices, payment links, marketplaces and small customer lists. A realistic phishing section should include attacks where the owner or client is tricked into changing bank details, paying a fraudulent invoice or authorising a transfer.

Proposed change: Add a “payment-change verification” bullet: verify new bank details, invoice changes, urgent payment requests, gift-card requests and account changes through a trusted out-of-band channel before acting.

Comment 19 - Technical

Location: 3.3.2 Protect Your Business from Ransomware / 15

Comment and rationale: The ransomware section should also address cloud account takeover and data extortion without encryption. Rationale: A non-employer firm may be harmed even if local files are not encrypted. Attackers may steal cloud-stored customer data, threaten disclosure, delete SaaS records, alter storefront content or lock the owner out of business-critical accounts.

Proposed change: Add examples and mitigations for cloud/SaaS ransomware-like incidents: cloud file deletion, account lockout, data theft/extortion, malicious sharing changes and recovery through provider support, logs, backups, MFA reset and session revocation.

Comment 20 - Technical

Location: 3.4 Detect Function / 16

Comment and rationale: The detection section should provide more concrete, low-cost monitoring examples for solo operators. Rationale: Antivirus logs are useful but many non-employer firms rely heavily on SaaS and cloud accounts. Useful signals may already exist in account security pages, banking alerts, email settings, website admin panels and payment processor dashboards.

Proposed change: Add examples: enable new-login alerts; review mailbox forwarding rules; review OAuth/connected apps; check recent account activity; enable bank/payment transaction alerts; review admin users on websites/storefronts; monitor domain/DNS changes; and check for unexpected password or MFA reset notifications.

Comment 21 - Technical

Location: 3.4 Detect Function / 16

Comment and rationale: The physical-security section should include mobile and shared-workspace realities for non-employer firms. Rationale: Many non-employer firms work from cafés, client sites, vehicles, homes, co-working spaces or temporary accommodation. Device theft, screen exposure, unattended sessions, public charging stations, insecure Wi-Fi and mixed family/business use are realistic risks.

Proposed change: Add practical steps: use screen locks, disk encryption, privacy screens where needed, device tracking/remote wipe, separate user accounts for family/shared devices, avoid unattended logged-in devices, secure laptops during travel and treat lost phones as a high-priority account-recovery incident.

Comment 22 - Technical

Location: 3.5 Respond Function / 17

Comment and rationale: The response guidance should include preserving evidence and avoiding compromised communication channels. Rationale: During an incident, a sole operator may continue using a compromised email account or device to seek help, notify customers or reset passwords. That can worsen the incident or alert the attacker. Basic evidence preservation also helps responders, insurers, banks or law enforcement.

Proposed change: Add a simple first-response note: do not delete suspicious messages; take screenshots; record times and actions; avoid using suspected-compromised devices/accounts for recovery; use a known-clean device where possible; revoke sessions; and contact banks/providers quickly for account or payment-related incidents.

Comment 23 - Technical

Location: 3.6 Recover Function / 18

Comment and rationale: The recovery guidance should emphasise validating account and cloud-service integrity before restoring normal operations. Rationale: Recovery is not only restoring files. Attackers may leave persistence through email forwarding rules, new admin users, malicious OAuth grants, changed recovery details, modified payment details, altered DNS records, website backdoors or new API keys.

Proposed change: Add guidance to review account recovery details, active sessions, MFA settings, forwarding rules, OAuth grants, admin users, payment details, DNS/domain changes, API keys, website plugins and cloud sharing settings before declaring recovery complete.

Comment 24 - Technical

Location: Appendix G / 35-37

Comment and rationale: The asset and risk worksheets are useful but should include treatment tracking fields. Rationale: A list of assets and risks is only actionable if the owner can decide what to do next and when to review it. Non-employer firms need lightweight tracking that turns risk identification into action.

Proposed change: Add optional columns for current control, planned treatment, treatment owner, due date, review date, residual risk, backup status, MFA type, recovery method and “can this asset reset or control other assets?”

Comment 25 - Technical

Location: Appendix H / 38-39

Comment and rationale: The Respond and Recover worksheet should include provider-specific contacts that reflect modern small-business dependencies. Rationale: A sole operator may need to contact more than law enforcement, legal, bank, insurer and a technical contact. The first hour of a real incident may require rapid action with an email provider, domain registrar, web host, payment processor, marketplace, cloud storage provider or accounting platform.

Proposed change: Expand the sample contact table to include email provider, domain registrar/DNS provider, web host/storefront provider, cloud storage provider, payment processor, accounting/tax platform, password manager emergency support, social media/business page support and client/customer notification contact list.

Comment 26 - Technical

Location: Appendix I / 40

Comment and rationale: The authentication worksheet should record MFA type and recovery posture, not only whether MFA is enabled. Rationale: “MFA enabled” can hide meaningful differences between SMS, email OTP, authenticator app, push approval, passkey, hardware key or backup codes. Recovery methods can be the weakest part of the account.

Proposed change: Add columns for MFA type, phishing-resistant MFA enabled, backup method, recovery codes stored securely, recovery email/phone protected, account has admin privileges, connected apps reviewed and last review date.

Comment 27 - General

Location: Appendices C-E / 25-33

Comment and rationale: The notional scenarios are useful but they would benefit from an example focused on a solo digital service provider or software/creative worker. Rationale: Many non-employer firms operate through repositories, source code hosting, design files, client portals, email, cloud drives, CI/CD systems, app stores, analytics tools and AI-assisted workflows. These firms have different risks from the lawyer, e-commerce seller and business consultant examples.

Proposed change: Add or adapt a notional scenario for a solo software developer, web designer, creator or digital services contractor. Include risks such as source-code leak, repository takeover, API-key exposure, client credential handling, cloud billing abuse, domain/DNS compromise and malicious dependency or plugin updates.

Comment 28 - General

Location: Supplemental Content / Appendices / ii, 34-40

Comment and rationale: The appendices would be more usable if released as companion editable templates. Rationale: The worksheets are valuable but many non-employer firms will not recreate tables from a PDF. Editable XLSX/CSV/ODS templates would make it more likely that owners actually complete inventories, authentication reviews, incident contacts and legal/contractual requirement trackers.

Proposed change: Publish companion downloadable templates for Appendix F, Appendix G, Appendix H and Appendix I in spreadsheet formats. Include example rows and a blank version. This would reduce friction for the intended audience and align with the document’s practical, low-resource focus.